Schneier on Security

NSA on Securing VPNs

The NSA's Central Security Service -- that's the part that's supposed to work on defense -- has released two documents (a full and an abridged version) on securing virtual private networks. Some of it is basic, but it contains good information.

> Maintaining a secure VPN tunnel can be complex and requires regular maintenance. To maintain a secure VPN, network administrators should perform the following tasks on a regular basis:
>
> - Reduce the VPN gateway attack surface
> - Verify that cryptographic algorithms are Committee on National Security Systems Policy (CNSSP) 15-compliant
> - Avoid using default VPN settings
> - Remove unused or non-compliant cryptography suites
> - Apply vendor-provided updates (i.e. patches) for VPN gateways and clients

Tags: cryptography, cybersecurity, NSA, security analysis, VPN

Posted on July 15, 2020 at 9:29 AM • 31 Comments

Comments

Stephen Craven • July 15, 2020 9:48 AM

I had never heard of the CNSS policies before so I tried to download them from https://www.cnss.gov/CNSS/issuances/Policies.cfm

On my Mac I get a "Your connection is not private" error on that policy page because it claims "www.iad.gov" certificate is not standards compliant.

Anyone else have this issue or understand the root cause?

Seems silly that the Committee on National Security Systems would have an invalid cert.

David Kowis • July 15, 2020 9:55 AM

The CNSS site is behind a US Gov't DoD Cert. Not a typical CA Bundle commercial cert.

Not sure how to get that root cert tho.

Search

Powered by DuckDuckGo

Go

● blog ○ essays ○ whole site

Subscribe

About Bruce Schneier

I am a public-interest technologist, working at the intersection of security, technology, and people. I've been writing about security issues on my blog since 2004, and in my monthly newsletter since 1998. I'm a fellow and lecturer at Harvard's Kennedy School and a board member of EFF. This personal website expresses the opinions of neither of those organizations.

Related Entries

- Former FBI General Counsel Jim Baker Chooses Encryption Over Backdoors
- Breaking Diffie-Hellman with Massive Precomputation (Again)
- Policy vs. Technology
- A New Clue for the Kryptos Sculpture
- Critical Windows Vulnerability Discovered by NSA

Bufford • July 15, 2020 10:18 AM

IF you trust the NSA to give advice that makes their job harder...

---

wiredog • July 15, 2020 11:14 AM

Installing DoD Root Certificates

Stephen Craven • July 15, 2020 11:15 AM

For those who care to see the CNSS policy without trusting an invalid cert, I found it posted on AWS: https://imlive.s3.amazonaws.com/Federal%20Government/ID151830346965529215587195222610265670631/CNSSP15.pdf

---

Shameless-Plug • July 15, 2020 11:21 AM

Any thoughts about Disconnect?

https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking

https://www.washingtonpost.com/technology/2020/07/13/tiktok-privacy/

---

fastcat • July 15, 2020 12:00 PM

> Avoid using default VPN settings

The fact that this has to be on the list sounds like an industry failure. VPN software sounds like the kind of thing that should always default to a secure configuration.

But also, this piece of advice is vague almost to the point of being useless. What default settings are they worried about? The document goes into this a *little*, mainly just saying that you should watch out for the default configurations allowing more cipher suites than you want. Which means it's basically a duplicate of the prior bullet.

Clive Robinson • July 15, 2020 1:12 PM

@ fastcat,

> VPN software sounds like the kind of thing that should always default to a secure configuration.

Kind of but...

The person providing the product does not want the expense of supporting it, nor do they want to put of potential sources of income.

Therefore the "default settings" are going to be "all things to all men" which in turn means there is lots of wriggle room for insecurity (such as exfiltration of information to third parties).

Thus the first thing you should do with a VPN is dump the generic all things settings and come up with a set tailored to your specific narrow requirments as this cuts out a lot of the wriggle room.

If an organisation can not do this because they either do not know how to, or their requirments are not narrow, then VPN technology is something that's probably unsuited for their needs and is an unnecessary cost.

Historically VPN's were not realy about security but traffic managment and what became "Quality of Service"(QoS). When you actually a lot of their usage they realy do not offer much in the way of security because as with any communications channel much of the security issues are at the end points.

Many people I know who use VPN's are not using them for their security but to avoid the poor security of other people. That is they use them to appear to be from some other location / address than they are at so they can gain access to services that they would otherwise not get.

For some reason "VPN" has become a "Managment Buzz Acronym"(MBA ;-) that goes on some checkbox list from some group or other that is "just going through the motions" for the sake of appearances.

Featured Essays

- The Value of Encryption
- Data Is a Toxic Asset, So Why Not Throw It Out?
- How the NSA Threatens National Security
- Terrorists May Use Google Earth, But Fear Is No Reason to Ban It
- In Praise of Security Theater
- Refuse to be Terrorized
- The Eternal Value of Privacy
- Terrorists Don't Do Movie Plots

more essays

Blog Archives

- Archives by Month
- 100 Latest Comments

Blog Tags

privacy / surveillance / terrorism / squid / academic papers / hacking / national security policy / NSA / cryptography / encryption / air travel / essays / law enforcement / malware / DHS / Schneier news / economics of security / crime / homeland security / vulnerabilities / fraud / computer security / TSA / laws / courts / police / cell phones / psychology of security / authentication / passwords

more tags

Latest Book

BRUCE SCHNEIER
BEST-SELLING AUTHOR OF DATA AND GOLIATH
CLICK HERE TO KILL EVERYBODY
Security and Survival in a Hyper-connected World
OK

more books

I Support Bloggers' Rights!

Defend Privacy Support EPIC

They come up with such lists by studying others "best practice"... That is they look at those things organisations who claim to be secure are doing. More specifficaly it will be the "Top Ten" organisations in some industry study by an industry media or group organisation that sells subscriptions or membership to "seniors" in other organisations.

As such "best practices" rarely have substance behind them, technically or otherwise, it raises the question of how much they are "magic umbrella thinking". That is not provable "cause and effect" (which you could only determin from a detailed analysis of each configuration and usage, which never gets mentioned in the articles or lists).

Jaime • July 15, 2020 2:53 PM

VPNs have been at least partly about security for a long time. Related to your endpoint comment... the most effective VPN products can be configured with "admittance criteria", meaning that the VPN won't connect unless the endpoint passes a series of checks. Good VPN software also prevents pass-through access. This is why you can't browse the Internet while connected to most corporate VPNs - they don't want to create an unprotected path from the Internet into the corporate network.

ANTI-Spy • July 15, 2020 6:13 PM

NSA, CIA, etc.. are all running paid VPN services like PIA (Private Internet Access).
When this happened:

https://wwwDOTyoutubeDOTcom/watch?v=DC10fyQgNqo

PIA IMMEDIATELY trashed their VPN server in Russia.
NOT a coincidence!

---

echo • July 15, 2020 8:52 PM

The only reason I use a VPNis to dodge past some irritating bureaucratic hurdles created by failed government initiatives and poor quality law and bootlicking executives looking for a bung creating "corporate made law" orthoganal to the actual body of law and democratic oversight. I leave it as an exercise to the reader to work out what I just meant.

My personal security policy is least effort swiss cheese. I keep one eye on the state to ensure it is behaving and play nod along with the crap installed on my laptops knowing full well it is only secure enough not to protect me but to indirectly protect them from their opposite numbers. Pretty much everything on my computers is a known known to the state level entity and with varying degrees to others at the same level depending on how nosey the relevant jobsworth is and whatever the arbitrary threat assessment is. My priorities are fairly well known and I don't have anything considered a secret although the combination of material and how it is used depending on the knowledge and skill and wetware between my ears is another story and this is not stored on the laptop. It's as much use as a pot of paint and artists easel is to a random chimpanzee i.e. not very.

In fact I'd go so far to say that any traffic analysis or end runs of my laptops would have said jobsworths shifting uncomfortably in their seats because they would have to get off their widening backsides and sort out the bureaucratic messes their political masters have created. If they did it would actually be a bonus so snoop away boys!

If I was serious about VPNs I'd run my own from home for the rare instance I use mobile internet but then I never use anyone elses wifi even if it is "free" so this is a moot point. I can be cheap but laziness overrides cheapness and I gain security by default even if it costs more. But oh noes the TLas may have hijacked my mobile telecoms providers infrastructure. If they have I'm stuffed anyway but honestly I don't want to spend my whole life glued to a screen. It'smore fun and better for my mental health to leave it switched off and enjoy view or people watching or simply fall asleep. Like Clive, I suspect, I have developed habit of being able to fall asleep in certain situations as an energy conservation scheme for when you need mental alterness. Not that I will be bungee cording off rooftops anytime soon but a reptile brain trained by situations and adversity is its own boss and that's not a fight I'm going to win even if somebody wheels in a free food trolley.

I suspect anyone intelligent knows the NSA or GCHQ et al may give out advice butit is advice working up to a box tick. It may be good as far as it goes but it goes as far as it goes for a reason. Those reasons may be political or a matter of communication or unstated purposes. One of those purposes is the projection of "authority" but "authority" like power is a variable and liquid and evasive quantity.

Bertrand Russels essays on power and laziness are worth reading. While his interviews on youtube are dated and of their time his reasoning is also extremely modern and very very relevant to the world we live in today much like the work of Welchman and Turing, I suppose, alongside a laundry list of other greats like Hopper and Lamarr which we can all gaze on with wistful irony.

I know we're living in somewhat fraught and chaotic times but I do wonder if a generation or so on whether anyone perhaps not yet born will be looking back on today and remarking of the greats. It would be nice to think so in spite of the volume of stupid but then everybody probably thought that all the way back to Roman or Babylonian times. As we begin to tease at the edges of what conciousness is perhaps even security in an information theory context I wouldn't be surprised if some wag in an ivory tower writes an essay on the raging discussions being had in the primordial soup. Oh, no you don't want to use that volcanic pipe because the big rock god might have backdoored it and you had better watch out for the amoeba at number 57 because they look funny.

It is rather funny that all this discussion is simply local energy systems within a greater context of a perceived universe whose current energy is a just a fraction of a fraction of a fraction above zero.

But yes various desks thumpers and hangers-on on the make have conspired and decreed accidentally or otherwise that VPNs are to be a thing so here we are carrying the Ju-Ju on its carriage from here to there. The crowds gather to merryily cheer it on its way and feed its spirit with confetti like coloured plastic symbols called "credit cards". All hail the Ju-Ju. There is none like the Ju-Ju. Praise be to the Ju-Ju.

Michael Salmon • July 15, 2020 11:30 PM

The Federal Bridge CA appears to have too long a validity, the limit set by the CAB Forum is 825 days, the above certificate is valid for a little over 3 years.

P/K • July 16, 2020 12:48 AM

The Central Security Service (CSS) actually consists of the Service Cryptologic Components (SCC) of the United States Armed Forces involved in signals intelligence, cryptology, and information assurance at the tactical level:
https://en.wikipedia.org/wiki/Central_Security_Service

The NSA branch that is responsible for defense is the Information Assurance Directorate (IAD), at least that was the name before the most recent reorganization. See also:
https://www.electrospaces.net/2014/01/nsas-organizational-designations.html

---

RealFakeNews • July 16, 2020 1:10 AM

Ever since the IPSEC backdoor scandal that hit OpenBSD, and the fact no-one has found a way to address covert subversion of crypto by either the crypto designer or software dev implementing it, it all seems rather pointless.

One minute the sec services are saying "do x, y, z" to secure something; next minute they're running said service in order to compromise it.

I can only assume they've caught the opposition with their hand in the cookie jar, and they're telling people how to block them without admitting anything.

Changing a few config settings in what is still a fundamentally back-doored security product is, IMHO, rather pointless.

As has been mentioned countless times on this blog, these apparently ineptly designed and written products are more likely to be deliberate.

There may be countless dumb people in the world, but I find it incredulous that the few smart people out there (who I'm sure are smarter than I), can't figure out how to write security software that is both secure AND easy to use. I'm still of the opinion that the lack of such products isn't coincidence.

RealFakeNews • July 16, 2020 1:20 AM

> Verify that cryptographic algorithms are Committee on National Security Systems Policy (CNSSP) 15-compliant

After DUAL_EC_DRBG, how can we be sure any of these are secure?

Something is just wrong with all of this.

Clive Robinson • July 16, 2020 4:36 AM

@ RealFakeNews, ALL,

> After DUAL_EC_DRBG, how can we be sure any of these are secure?

We can not and we would be daft to do so. After all as someone once noted,

> The price of freedom is eternal vigilance.

When taken with the older,

> Keep your friends close but your enemies closer.

Gives rise to a mind set that would be close to paranoia if it was not for the fact "The bugg3rs realy are out to get you".

But lets take a step back and look at the historical context. The earliest forms of "security" were through some form of obscurity, learnt from observing food prey.

As we in theory became more sophisticated we learnt the advantages of secrecy, again through food and water sources.

Eventually we learnt to communicate in an abstract way and the value of information became apparent as well as the value of information in transit.

Thus we developed what became codes. Unfortunatly codes are vulnerable to observation which is perhaps not that supprising as it appears that is how we learn to talk.

Thus the idea of ciphers came into being and again by observation we came up with new ideas to defeat them. Over several millennia we eventually arived at ciphers that could not be meaningfully broken. The OTP if made and used correctly leaks only that a plaintext message is not longer than the ciphertext.

But for good reasons we moved from difficult to use pencil and paper ciphers to mechanical cipher machines some of the simplest were designed a millennium or so ago, but it was not till the standardisation of mechanical parts in the late Victorian period (Whitworth threads) that more complex machines could be built. But within almost a life time they became obsolete, mechanics are not upto the complexity of electronics. But we've found that there are things such ciphers can not do...

It's less than a century since the first mathmatical (Hill[1]) ciphers were developed into a usable form. However whilst mathmatics is giving us numerous new possibilities, we don't yet know enough about mathmatics to spot the more subtle issues at design time. Thus in a way we are back in the time of Ceaser comming up with new ideas, and others are finding holes in them to get at the secrets within.

[1] In 1929 Hill and a partner developed a mechanical cipher based on multiplying matrices. This is based on linear algebra and on it's own is fairly weak. But it does provide good diffusion which is why you find the use of matrix multiplication in both Twofish and AES.

Who? • July 16, 2020 6:06 AM

@ fastcat, Clive Robinson

Sometimes avoiding the "all things to all men" approach is good. Think, for example, on OpenBSD and its "secure by default" settings. At that time software manufacturers were releasing anything in an "open by default" state so all was just working. The OpenBSD approach, instead of implying an increase of work for system administrators, supposed much less time spent hardening a widely open by default fresh system installation.

Of course, choosing the right algorithms for a VPN has two serious drawbacks, so the "secure by default" approach may not work for this technology:

1. these secure algorithms change over time; new algorithms are developed while others are dropped as weaknesses are discovered/published, opening a serious interoperability problem.
2. secure algorithms are, usually, slow. Performance is a key measurement when investing on a new technology, think on Intel and how it sticks to unsecure technologies instead of developing a line of secure —predictable— but slower processors. **Security sells, but not as much as performance.**

I want to take this opportunity to talk here to acknowledge the NSA for its great work on these public CSIs, CSAs, CSRs, CTRs and ORNs. All these are great documents, as said before full of common sense and good practices, that make the world safer. Keep up the good work!

Clive Robinson • July 16, 2020 12:19 PM

@ Who?

> All these are great documents, as said before full of common sense and good practices, that make the world safer.

Sadly the "defensive" side is a very small part when compared with the "offensive" side.

Worse from what we can tell they are often kept in the dark by the "offensive" side.

Basically the argument is that the "offensive" side is what brings home the intel... All be it more from "allies", friends and citizens rather more than it does others... Because the reason is that allies, friends and citizens have the infrastructure that makes "offensive" behaviour possible.

Not being funny but many second and third world nations do not have basic infrastructure outside of a few areas thus more advanced infrastructure such as is required for effective connectivity the offensive side can use is lacking.

So the question arises as to what intel allies, friends, and citizens can provide that is so important that over 2/3rds of the non admin staff are involved with it?

Well there could be many answers one of which is "industrial espionage" another is "nothing worthwhile". In either case I suspect that most of the citizens I suspect would rather the money be put to something more usefull.

The problem though is that if the "defensive" side were shall we say more helpfull, then any improvments they make will work not just for the citizens but also for those of other nations. Thus will work against the "offensive" side...

The reality is that this document says next to nothing above what a good admin should already know[1] or can easily find out if reading many manufactures upto date literature.

Which is a shame, because it's reasonable to assume that the defensive side is actually way more knowledgeable, and they are in fact "dumming down" a lot. Effectively to below what is already "public knowledge" but not of necesity widely so.

[1] There is one part where some might disagree which is recomending CBC as the encryption mode at the network or link level... Whilst CBC is good "general" advice for those who are not familiar with the intricacies of crypto algorith modes and high reliability networks. There are in less reliable networks and some specific cases liked fixed data rate applications other modes that are better. Especially with effectively fixed low bandwidth or unreliable networks such as RF links where repeates due to drop outs and other effects where the BER drops below 1 in 10^6 or even 10^2 can be an issue (encrypted speech on analog lines can be quite problematical and CBC just will not work when other modes will).

Who? • July 16, 2020 3:11 PM

@ Clive Robinson

You know, I completely agree with you. The NSA is the intelligence community Janus, looking at the past bringing home intelligence from both adversaries and allies and to the future too, when improving the security of networks.

Sometimes the behaviour of the NSA is difficult to understand——e.g. while spying allies such as Angela Merkel, a behaviour that only matches an agency doing industrial espionage against an adversary, something the NSA should never do both because they are in the business of protecting a country, not gathering industrial knowledge from foreign corporations, and because Europe is supposedly an ally of the United States.

However I like getting out the best of people and I really appreciate these documents. Should the two-faces NSA be splitted in both a defensive and an offensive agency? It is not clear to me. I am sure the former would have serious burocratic challenges making its work public. On the other hand, being good in the offensive side helps the defensive aspect of its work.

I agree with you, there is nothing unknown to a competent system manager on these documents. This one is, in a generic way, my ruleset for hardening an ISAKMP/IKE VPN using iked(8) in OpenBSD:

```
pass in on egress proto udp from any port > 1023 to self port isakmp
pass in on egress proto udp from any port > 1023 to self port ipsec-nat
pass in on egress proto esp from any port > 1023 to self
```

It matches exactly the rules suggested in these CSIs. But it is an effort in the side of the NSA to do the right thing, and it is something I appreciate. Does it mean I trust the NSA? Obviously not. I have the habit of never trusting these persons and entities that do not trust on me, not to say I am a very private person and heartly dislike the way NSA conducts its global surveillance against allies.

At the end, as Henry Kissinger said, there are no allies only shared interests.

---

echo • July 16, 2020 4:42 PM

@Clive @Who

I have great difficulty comenting on what you are writing because my mind immediately translates everything into the equivalent human rights and social systems. Yes I understand all the systems and technology stuff it's just not my focus and it's a real struggle to connect with solely IT systems discussion.

Irritatingly I have the same problem but opposite with women in IT. Why is every women's IT conference about women's subjective experience in the workplace and complaining about being sidelined? I'm left screaming "Where's the IT?"

On the issue of US security policy Bill Clinton issued an "executive order" that US military and intelligence were to deploy their assets in pursuit of US economic interests. I have read comment which suggests this policy was always implied which makes Bill Clintons executive order redundant. The doubling down by the Trump regime over the past few weeks and months is simply a continuation and escalation of the underlying schemes.

I'm curious why nobody has picked up on the head of MI6 talking a load of nonsense about policy changing when the facts changed. The security issues and facts have not changed. What has changed is the weakness of the UK government buckling under their own arbitrary and unwritten economic priorities. Effectively, the UK is now a second or third world nation. If Lord Neubergers comments on the UKs UN legal obligations are anything to go by if the UK is selling out human rights treaty obligations as both the UN and EU assert then the UK is not fit to hold a permanent seat on the UN security council. What does the revolving chair head of MI6 and his ex security service chums have to say about this?

What is it about office politics and organisations which leads to an erosion of standards?

I know this is veering wildly off the subject of VPNs but I feel the basic technicalities, what the manual says, and the role of a VPN are no different in practice to other systems which require secure endpoints. The fact Marcy Wheeler felt the US is so unreliable she had to move to Ireland is what I feel about the UK. Do we all have to VPN to an endpoint within the EU?

Clive Robinson • July 17, 2020 2:44 AM

@ echo,

> Why is every women's IT conference about women's subjective experience in the workplace and complaining about being sidelined? I'm left screaming "Where's the IT?"

I suspect the reason when you get to the bottom of it is "economic security".

That is at times of economic unrest which we have been in since before Financial Crisis One (FC1) every one in ICT is looking over their shoulders as to who is going to get that Human Resources chat before being escorted of the premises.

Put simply managment view ICT as a necessary evil to do business but also as sunk costs, which is money they would rather use for other things. We've seen the SysAdmin industry go from self taught experts who could get the best out of every bit of kit to "button push kids" who have lots of certificates from the equipment suppliers. As these are now more numerous than "mailroom workers" various people thing that they should be paid the same...

The more recent change is not industry issued qualifications but academic issued qualifications. Whilst I have the latter I nolonger have the former. In theory academic qualifications are not just independent but have depth and breadth as well as a research element. This has evened up the equitable pay issue, as some ICT people are more highly qualified than the managers, and some have even got themselves business qualifications as well.

Thus unsuprisingly people who are not just well qualified but quite inteligent want more equitable renumeration and can get with a little care and hard barganing get it. However the more traditional managment see them as little more than "blue collar workers". Understabdably this creates both tennsion and unrest.

Without going into the whys of which there are many women are generaly more vulnerable not just in the work place but in society and legaly as well, and quite rightly many women feel that it is wrong.

Thus women in ICT genuinely have good reason to fear the uncertainty and what it does to their "economic security".

But confrence organizers likewise have their own worries not just in these times of economic unrest but more so in that they have to invest quite heavily up front for venues etc. Thus they are going to be keen to get people through the door which means that in reality they have to appeal to "common denominator thinking" to ensure their own economic security.

One of the reasons I stopped attending conferences and seminars was they were all becoming "shows" to push product etc. Whilst I can understand the desire to do this it's also my money and time I'm investing. Thus as I was not getting what I thought was a fair deal I found better things to do with my time and money.

It's interesting to note that most of those conferences and seminars now nolonger exist. I suspect the reason was that they tried to "over profit" and as a result others "voted with their feet" and stopped going due to lack of relevance, thus a tipping point was reached...

Which is what has happened in the UK and one of the results is the UK Government has to do as it's told by everyone if it hopes to reach trade deals, which I suspect are going to be very unfavourable no matter how hard the polititions "polish the turd" that is the mess the UK is now in and they will not stop digging to make it worse... Thus the recent anouncment made about a certain Chinese Telco[1].

Which brings us back to communications security,

> I feel the basic technicalities, what the manual says, and the role of a VPN are no different in practice to other systems which require secure endpoints.

A VPN when all is said and done is a "Shannon Channel" which fundementally makes it little different to two tin cans and a tight bit of thin string between them. Historicaly it's purpose was not security but dependable traffic managment to ensure "Quality of Service" between two points. At some point people wanted to route traffic from one point of their organisation to another across private networks on leased lines from public entities. For some people the lack of "security" worried them so they developed "armouring" one such way was to use two "Bastion Hosts" and "stunnle" or similar.

But as with all usefull things people wanted to use it for other reasons so the goal posts kept moving with the resultant "feature creep and non standardisation". Thus somebody put forwared the idea if IPsec which instead of making things simpler made them worse a lot worse especially when VPN's got routed across other VPN's and similar.

One upshot is that VPN's are frequently not "point to point". That is one end of the VPN is inside the organisation and there are ten or more "remote clients" out in the Internet somewhere, often without fixed IP addresses.

Few people can instinctively get their heads around the implications of this and with manufacturers trying to make their products easier to use actually make things a lot worse, almost back to the mayhem prior to IPsec.

Which brings me back to the point about manufacturers qualifications. Managing complexity effectively is not something humans are particularly good at. So manufacturers impose their idea of what is required and build it into "push button" tools. There is no agrement between manufacturers as to the "what and the how" of their tools, in fact it's seen as being in their interests not to. Thus to get two different manufacturers kit to talk has often ment throwing the tools away and dealing with very raw low level interfaces which again are not standard. Finding out how to do this is not something the manufacturers realy want you doing for a whole host of reasons not least of which is changing the low level interface without warning. Thus things get broken, sometimes invisibly.

But at the end of the day, having a VPN into an organisation with the other end being open to the Internet is not the best of ideas, but the drive to reduce costs makes this inevitable. Likewise the same cost reduction drive means skilled labour is replaced with what is effectively unskilled labour "following a recipie book" to get a solution and frequently failing to do what is actually required. Especially when those involved realy do not understand security at a fundemental level, something you only sometimes get on academic courses, not manufacturers training...

[1] The latest reasoning is as ludicrous as previous reasoning and none of the accusations or in this case illusions actually hold any water. For instance most antennas are pasive and even those such as "phased array" are not exactly going to have the ability to somehow mysteriously beam secrets to China. Likewise a lot of other equipment. Thus a spurious reason has been invented for US political purposes and it's going to cost the UK upwards of 3-5billion dollars as well as forcing highly undesirable single source supply lines and the like which realy do threaten National Security.

---

echo • July 17, 2020 4:16 AM

@Clive

I see things a little differently in the sense that abuse of power and comfort zones in the form of sex discrimination and holy huddles tends to push a "no change default". There is a whole stack of neuro-psycho-sociology on this not to mention organisation theory. The media also have major issues covering thisproperly as largeswathes of them aresimply not capable of holding their attention span for more than five minutes and most academics tend to live intheir ivory towers where a lot of sexism is still rampant. You can also see the way media narratives are twisted in interviews with male and female actors. Men get to discuss their acting challenges and accomplishments whereas interviews with women are often framed as more autobiographical struggles.

I've given up on IT as there's no way back into the industry at my age and I have no interest in an industry led by products rather than what they are supposed to achieve and everything including the kitchen sink application frameworks. Nobody wants to hear my views on application architecture or game design because they are old farts too busy being macho and peddling their books or simply young and on another planet. I'm not criticising their work or their technology analysis which was actually rather good but simply there was a point of view or age gap. As for conflicting and closed standards. Let's not go there. The whole corporate and marketing tilt excludes and silences a lot of views simply because,I suppose, because of the self-fulfilling economic angle you mention but I can't help thinking they are missing something. It's all there and the talent and energyis there. It's just I feel the focus of effortis somewhat misapplied.

The whole "Lean In" philosophy has been discredited because of various discredited dogmas but I personally think simply a little more focus on IT would help.

The UK government almost disbanded the SAS but they made it their business to make themselves useful. Now I don't think being pushy or feature creep help much but again there is a focus on function. The SBS lagged quite a lot until they have a new CO and changed their focus and I gather they reached parity then a reorganisation of special forces took place and everything knits together rather well. So change can happen but it requires more than just technical changes and I think this is what IT and other industries and personnel aren't quite getting at the moment mostly due to emotional issues and fears of personal irrelevance.

I've visited a few trade shows but this was years ago before half the people working in the industry were born. Like yourself I noticed most of them have disappeared. God knows what goes on at defence shows but given comments from a narcissistic marketing consultant paid far too much money with an ethical bypass I discussed a few things with I have a suspicion "face not fitting" syndrome would kick in very rapidly.

As for VPNs they have a small role in my least effort house of cards made out of Swiss cheese. I don't think about them any deeper than that. I guess they are yet another fashionable ponzi scheme with the usual dodgy fingers in the pie.

Oh, on the issue of telco phased arrays we of course know that traffic analysis include meta data can be useful but also the phased arrays add not just cell location or distance to phone information but now the possibility of direction information. I'm curious why you have never commented on this.

Weather • July 17, 2020 5:06 AM

@echo
I would like to hear your though on phase array antenna, thanks

---

echo • July 17, 2020 5:41 AM

@Weather

It's nothing special. 5G towers include the ability use their arrays to direct a signal left or right towards a phone to provide a stronger signal. I just think direction and distance narrows down the location or may provide movement data. What actually happens inside the tower and what data is passed on and what use it may be put to I leave for others to work out.

I'm not too bugged about it myself at an individual level. Nothing can be learned that couldn't be found out other ways.

Clive Robinson • July 17, 2020 7:27 AM

@ echo,

> on the issue of telco phased arrays we of course know that traffic analysis include meta data can be useful but also the phased arrays add not just cell location or distance to phone information but now the possibility of direction information. I'm curious why you have never commented on this.

Untill 5G phased arrays were not realy part of mobile phone technology, so it was not realy relevant untill recently.

But you atleast are aware of the important point,

> I'm not too bugged about it myself at an individual level. Nothing can be learned that couldn't be found out other ways.

Those "other ways" are how the antenna controler gets told where to point the beam.

Under several not that infrequent circumstances the cellular technology actually knows your position rather better than any GPS unit in the phone.

Whilst "direction" and possibly "range" are important to a 5G mast and it's phased array antenna, it's of little importance to LEO and IC agencies because they want lat/long of position.

With 4G and LTE that "position information" is not actually known but calculated in various ways and will be the same for 5G initialy.

Unfortunately there is a dirty little trick that some unscrupulous prosecutors use... when presenting in court they give the position as if it's down to a pencil dot on the landscape. That is they fail to give the error margin which can be quite considerable and put you not just a road or two away but a couple of city blocks or more...

Richard H • July 17, 2020 9:07 AM

@echo @Clive et al:
Talking about "the beam" as though it were a single narrow unidirectional thing is misleading. Phased arrays for 5G etc. (incidentally it's not true to say this is new with 5G, phased arrays and MIMO are used in HSPA and LTE) are not trying to solve the problem "where is the phone?" but "what combination of these antenna phases and amplitudes gives the best data rate over this collection of channels?" which is at least one step removed. From an RF engineering viewpoint, there is no single "direction" and the "beam" is probably a continuously-changing overlapping fan of many lobes.

With the ability to solve that problem in real time, what used to be a problem (dispersion due to multipath) is being turned into a solution (spatial-frequency diversity supporting multiple independent channels using MIMO).

(Incidentally the phone itself may well be using adaptive beamforming techniques to steer its own antenna, to cancel the radiation from noisy on-board components, so there are more variables than you might expect in this equation.)

---

lurker • July 17, 2020 12:47 PM

@echo, et al,

> 5G towers include the ability use their arrays to direct a signal left or right towards a phone to provide a stronger signal.

Strong enough according to some misguided souls, to damage human tissue. But on the question of the steering metadata being collected by 3LAs, for now I'd rather my secrets went to China than to the Pentopticon.

---

echo • July 17, 2020 3:43 PM

@clive

I never thought about it that way around. Thanks.

I don't actually care that much about mobile technology in general being able to snoop and track. There really isn't much they could discover which couldn't be found out other ways.

Position and direction in combination with map and profile data can narrow down the circle of probability which is the position the prosecution would becoming from. There is also all the other data which excludes everyone else so the probabilities narrow again. As we know if there is a means to collect data from more sensors probabilities narrow accordingly as the definition and uniqueness of the fingerprint increases. You can see the granularity increase from possibly in the area to target located in the building to having an inside source inside the walls. But they still have nothing other than the possibility of a target or a hooning idiot in the wrong place at the wrong time.

It's one of the oldest tricks in the book to maintain a pattern and act unseen outside of the variables.

Forensics and intel can also be bad at detecting indirect influences or influences where perception plays a role in identification. The "hidden hand" can often receive no more than a slap on the wrist or get off.

The only people who need to be worried are those who can't control their impulses, opportunists, and the careless.

I'm guessing this is why when Cameron attempted to bring in mandatory sharing of telecoms towers to do away with "blackholes" in service coverage GCHQ threw a hissy fit. They put ease of collecting the datastream before user convenience and telecoms infrastructure "fitting around the problem".

@lurker

Yes the conspiracy theorist stuff was nuts. There simply was no science supporting it. And speaking of the science by chance I discovered the other week that divers working on maintenance in water pools which shield radioactive components can receive less radiation than a person walking down the road receives from background radiation. Of course this depends on the type and intensity of radiation source.

Clive Robinson • July 17, 2020 6:54 PM

@ echo, lurker,

> I discovered the other week that divers working on maintenance in water pools which shield radioactive components can receive less radiation than a person walking down the road receives from background radiation.

The people up at the UK's Cellerfields nuclear reactors new about certain of Chernobal's effects long befor the public health officials.

The reason the radiation detectors there are so sensitive they detected the leading edge of the radioactive airborne cloud and raised critical alarms long long before the radiation got to the same level as a luminous watch dial half a meter from your head.

The accidental radiation overdose people you should feel sorry for are those working in the aviation industry. For instance mid this week a solar storm eminating from the sun hit the earth. It's intensity was such that anyone in the air inside a modern jet liner probably received a dose in a single flight that exceeds half a years maximum dose.

Thus it is almost certain that a number of people now have a cancer oportinity they did not prior to fiying.

echo • July 17, 2020 7:23 PM

@Clive Robinson

Yes, I vaguely recall hearing about Sellafields (a.k.a Windscale lol) detectors. For some reason it's one of those things which doesn't stick in my head. I suspect you are correct about the sudden burst of solar radiation affecting sky travellers. It's one of those reminders that we exist at the tail end of a lot of cosmological probabilities like a microbe living at the edge of a volcanic vent.

Apparently, the seismic detectors scattered about the UK are sensitive enough to detect an exploding grenade. When there was some news about the police catching one Herbert making homemade bombs and testing them on open land the story was the police were tipped off by a "man walking a dog". I didn't believe this at the time because the police have pulled this wheeze before. As things rolled on news later emerged this turned out to be a cover story and they had received intelligence from another agency. Whether this Herbert was caught by seismic detectors or an opsec leak or brazenly ordering a huge quantity of a "monitored" substance I have no idea but I always wondered.

Some unrelated context is Radio 5 early morning news was often very on the ball with stories which were massaged as the day went on until the bland establishment ass kissing version made its way to the evening news. There is also the phenomena of police and sometimes customs officers broadcasting operational details when they were fashionably interviewed in the carpark with a view of their HQ in the background until they were edited out of further coverage a few days later or, if they were really on the ball, by the time the evening news rolled around. Law enforcement is much better with containing their own leaks today than they were but as with all things the focus shifts somewhere else. The Dibbles have been caught with their hands in the cookie jar over no-criming, dodgy undercover operators, profiling, and various fudges and lack of internal and external scrutiny to cover up mistakes.

---

anon • July 18, 2020 8:00 AM

Odd how the #1 most-common screwup is completely absent (or, maybe not so odd, given who issued the advice?): client configuration.

Updates cut both ways too, remember. Maybe it's fixing a flaw. Maybe it's adding a feature. Maybe that feature isn't in your best interest...
https://www.theguardian.com/technology/2018/dec/08/australias-war-on-encryption-the-sweeping-new-powers-rushed-into-law

---

Subscribe to comments on this entry

Leave a comment

Login

Name (required):

E-mail Address:

URL:

☐ **Remember personal info?**

Fill in the blank: the name of this blog is Schneier on ___________ (required):

Comments:

Allowed HTML: <a href="URL"> • <em> <cite> <i> • <strong> <b> • <sub> <sup> •   • <blockquote> <pre>

Preview **Submit**

← Enigma Machine for Sale

Twitter Hackers May Have Bribed an Insider →

Sidebar photo of Bruce Schneier by Joe MacInnis.